UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/927,928	08/09/2001	Rodric C. Fan	M-11702 US	6041

7590 01/04/2005

MacPherson Kwok Chen & Heid LLP
1762 Technology Dr.
Suite 226
San Jose, CA 95110

EXAMINER	
TESLOVICH, TAMARA	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/927,928	FAN ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *08.09.01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Publication 2002/0004898 (AC) Droge (U.S. Patent Application ~~09/841,168~~) and Schneier (Applied Cryptography, 2nd ed.). Schneier has been relied upon as a reference for features inherent to the Data Encryption Standard (DES).

As per claim 1, Droge discloses a method for transmitting data, the method comprising: encrypting a payload; adding a header to the payload to form a data packet; encrypting the payload and the header of the data packet so that the payload is at least twice-encrypted an the header is at least once-encrypted; transmitting the data packet only after at least twice encrypting the payload (see Droge figures 5 and 6).

As per claim 2, Droge discloses the method of claim 1, wherein the encrypting a payload further comprises: encrypting the payload with a symmetric key (see Droge paragraph 53 reference "DES").

As per claim 3, Droge discloses the method of claim 1, further comprising: receiving the data packet at a first device; performing a first decryption of the data packet that first device; forwarding the data packet to a second device; performing a second decryption of the payload at the second device (see Droge figure 6).

As per claim 4, Droge discloses the method of claim 1, further comprising: creating a symmetric session key; wherein the payload is encrypted with the symmetric session key (see Droge paragraph 53 reference "DES").

As per claim 5, Droge discloses the method of claim 1, wherein the transmitting further comprises: transmitting the data packet over a wireless link (see Droge paragraphs 36 and 40).

As per claim 6, Droge discloses a device for transmitting data comprising: a wireless transceiver (see Droge paragraph 36 and 40); an encryption engine coupled to the wireless transceiver for encrypting a payload according to a first encryption algorithm, adding a header to the payload to form a data packet, and encrypting the data packet according to a second algorithm (see Droge paragraphs 35, 39-41 and figures 5,6); a processor coupled to the encryption engine and to the wireless transceiver and configured to execute the encryption algorithms (see Droge paragraphs 35, 39-41 and figures 5,6).

As per claim 7, Droge discloses the device of claim 6, further comprising: a receiver coupled to the processor for receiving the data to be transmitted (see Droge paragraphs 39 and 53, figure 6 step 90).

As per claim 8, Droge discloses the device of claim 6, wherein the payload further comprises location information regarding the location of the wireless device (see Droge paragraph 58, reference "IP header").

As per claim 9, Droge discloses the device of claim 6, wherein the first encryption algorithm employs a symmetric key (see Droge paragraph 53 reference "DES").

As per claim 10, Droge discloses a method comprising: generating a symmetric session key at a first device; encrypting the symmetric session key at the first device using a public key associated with a second device; transmitting the encrypted session key to the second device; decrypting the encrypted session key at the second device using a private key associated with the public key; encrypting a payload using the symmetric session key at the first device (see Droge paragraph 50 reference "algorithms that might be used to encrypt data at [the link layer] includes, without limitation, the DATA ENCRYPTION STANDARD (DES)"); adding a header to the payload to form a data packet at the first device; encrypting the payload and the header or the data packet to form an encrypted data packet at the first device; transmitting the encrypted data packet from the first device (see Droge figure 6, steps 92-102).

As per claim 11, Droge discloses the method of claim 10, further comprising: receiving the encrypted data at a third device; decrypting data packet at the third device to form a decrypted data packet, the decrypted data packet having an encrypted payload; forwarding the decrypted data packet to the

second device (see Droge figure 6, steps 104-114); decrypting the payload at the second device using the decrypted session key (see Droge paragraph 50).

As per claim 12, Droge discloses the method of claim 10, wherein transmitting further comprises transmitting the data packet over a wireless network (see Droge paragraphs 36 and 40).

As per claim 13, Droge discloses the method of claim 10, wherein the first device comprises a wireless device and the second device comprises a wireline device (see Droge paragraphs 61-62).

As per claim 14, Droge discloses the method of claim 10, wherein the second device comprises a server (see Droge paragraph 60).

As per claim 15, Droge discloses the method of claim 10, wherein the payload includes location information (see Droge paragraph 58, reference "IP header").

As per claim 16, Droge discloses the method of claim 10, wherein the generating symmetric session key at a first device further comprises generating the symmetric key based on a random number (see Droge paragraph 53).

As per claim 17, Droge discloses the method of claim 10, wherein the encrypting a payload using the symmetric session key employs at least one fo the encryption algorithms DESX or DES (see Droge paragraph 53).

As per claim 18, Droge discloses a method for transmitting data, the method comprising: encrypting a payload using a first key; adding a header to the payload to form a data packet; encrypting the payload and the header of the data packet with a second key; transmitting the data packet (see Droge figure 5).

As per claim 19, Droge discloses the method of claim 18, wherein the first key comprises a symmetric key (see Droge paragraph 53 reference "DES")

As per claim 20, Droge discloses the method of claim 18, wherein the encrypting a payload further comprises: encrypting the payload using at least one of the encryption algorithms DES or DESX (see Droge paragraph 53).

As per claim 21, Droge discloses a method comprising: generating a symmetric session key at a first device; encrypting the symmetric session key at the first device using a public key associated with a second device; transmitting the encrypted session key to the second device; decrypting the encrypted session key at the second device using a private key associated with the public key; encrypting at least a portion of a data packet using the symmetric session key at the first device to form an encrypted data packet (see Droge paragraph 50 reference "algorithms that might be used to encrypt data at [the link layer] includes, without limitation, the DATA ENCRYPTION STANDARD (DES)"); transmitting the encrypted data packet from the first device (see Droge figure 6, steps 92-102).

As per claim 22, Droge discloses the method of claim 21, wherein the transmitting of the encrypted data packet further comprises transmitting the encrypted data packet over a wireless link (see Droge paragraphs 36 and 40).

As per claim 23, Droge discloses the method of claim 21, wherein the first device comprises a wireless device and the second device comprises a wireline device (see Droge paragraphs 61-62).

As per claim 24, Droge discloses the method of claim 21, wherein the second device comprises a server (see Droge paragraph 60).

As per claim 25, Droge discloses the method of claim 21, wherein the data packet includes location information (see Droge paragraph 58, reference "IP header").

As per claim 26, Droge discloses the method of claim 21, wherein generating a symmetric session key at a first device further comprises generating the symmetric session key based on a random number (see Droge paragraph 53).

As per claim 27, Droge discloses a device comprising: a processor (see Droge paragraphs 35, 39-41 and figures 5,6); a wireless transceiver coupled to the processor for transmitting an encrypted data packet to a server (see Droge paragraph 36 and 40); a memory coupled to the processor, the memory having a public key associated with the server permanently stored therein (see Droge paragraph 39); wherein the processor encrypts the encrypted data packet using the public key. (see Droge paragraph 53 reference "DES")

As per claim 28, Droge discloses a device comprising: means for encrypting a payload; means for adding a header to the payload to form data packet; means for encrypting the payload and the header of the data packet so that the payload is at least twice-encrypted an the header is at least once-encrypted; means for transmitting the data packet only after at least twice encrypting the payload (see Droge figures 5 and 6).

As per claim 29, Droge discloses a computer readable medium comprising program instructions for performing a method comprising: encrypting a payload; adding a header to the payload to form a data packet; encrypting the payload and the header of the data packet so that the payload is at least twice-encrypted and the header is at least once-encrypted; transmitting the data packet only after at least twice encrypting the payload (see Droge figures 5 and 6).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER